# POINTERS

## NSA nurtures growth of a science of security community

The National Security Agency (NSA) actively supports research to develop a scientific approach to cybersecurity. Currently, NSA has several initiatives to stimulate and encourage advanced work on the emerging field termed a science of security (SoS).

First, the Research Directorate announced the winner of the 2013 Science of Security (SoS) Best Scientific Cybersecurity Paper Competition in August 2014. The competition reflects the Agency's desire to increase scientific rigor in cybersecurity.



SCIENCE OF SECURITY

This year's winner, "Memory Trace Oblivious Program Execution," was a research paper presented at the 2013 IEEE Computer Security Foundation written by Chang Liu, Dr. Michael Hicks, and Dr. Elaine Shi. Their research centered on a scientific foundation for the use of oblivious random-access memory, or ORAM, in programs. Two aspects of the paper were compelling to the reviewers: First, it builds a bridge between cryptographic research and information flow research, and shows how the latter can help one apply cryptographic advances in a

principled and secure manner. Second, it establishes a scientific foundation for the use of ORAM in programs. It provides a valuable and exciting direction toward making ORAM practical.

Of the 35 papers nominated, one paper received honorable

1

mention, "Rethinking SSL Development in an Appified World" by Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, and Dr. Matthew Smith from the Distributed Computing and Security Group at Leibniz University in Hannover, Germany. Their paper was presented at the 2013 ACM Conference on Computer and Communications Security. The paper studies the possible causes of SSL problems on appified platforms. The results show that the root causes are not simply careless developers, but also the limitations and issues of the



NSA is funding SoS lablets at Carnegie Mellon University, North Carolina State University, the University of Illinois at Urbana-Champaign, and the University of Maryland to advance cybersecurity science. In this photo (from left to right): Mr. Gil Nolte, chief of NSA Trusted Systems Research; Dr. Jonathan Katz, principal investigator for the UMD SoS lablet; Dr. Laurie Williams, principal investigator for the NC State SoS lablet; Dr. David Nichol, principal investigator for the UIUC SoS lablet; and Dr. William Scherlis, principal investigator for the CMU SoS lablet.

current SSL development paradigm. The authors took an unusual step which was highly important—they systematically contacted developers who had produced insecure code.

Additional details about this year's competition can be found at the SoS Virtual Organization website (http://cps-vo.org/group/sos/papercompetition).

Second, NSA has become more involved in academic collaborations, such as the Symposium and Bootcamp on the Science of Security (Hot SoS), hosted in April 2014 by the North Carolina State University SoS lablet, and held in Raleigh, North Carolina. Hot SoS is a research event centered on developing an SoS that addresses the fundamental problems of cybersecurity. Cybersecurity has been intensively studied, but previous research often emphasizes the engineering of specific solutions without first developing a scientific understanding of the problem. All too often, cybersecurity research conveys the flavor of identifying specific threats and removing them one at a time. The motivation behind the nascent SoS is to develop basic cybersecurity properties using scientific rigor to understand how to determine trust in systems. At Hot SoS, researchers from all over the country presented 12 papers and 23 posters. These presentations can be found at http://www.hotsos.org/2014/ proceedings.html.

Third, NSA provided \$8.2 million in direct support to Carnegie Mellon University, North Carolina State University, the University of Illinois at Urbana-Champaign, and the University of Maryland for SoS research lablets. Within this program, each lablet (i.e., a small lab) will be conducting basic foundational research, building a growing community of researchers from multidisciplines and various universities, and championing the need for an SoS. They will be identifying scientific principles upon which to base trust in cybersecurity. The overarching goal is to bring scientific rigor to research in the cybersecurity domain. The research will focus on five hard problem areas: 1) scalability and composability, 2) policy-governed secure collaboration, 3) security metrics, 4) resilient architectures, and 5) understanding and accounting for human behavior.

### Carnegie Mellon University SoS lablet

The Carnegie Mellon University (CMU) SoS lablet addresses cybersecurity challenges related to all five hard problems with particular emphasis on scale and composability of modeling and reasoning, and human behavior and usability for developers, evaluators, operators, and end users. One anticipated result is progress in identifying and sharing the most effective theoretical and experimental approaches to address the scientific challenges within the five

hard problems. A second anticipated result is a better understanding of how to design and choose appropriate modeling abstractions in cybersecurity research. A third anticipated result is the identification of patterns and best practices in the way we carry out cybersecurity research, including approaches to data gathering, analysis, nomenclature, and means to promote reproducibility, enabling more rapid advances in the scientific field. Dr. William Scherlis is the principal investigator for the CMU SoS lablet.

The CMU SoS lablet projects include

- ▶ Safe programming languages,
- ▶ Binary and source code analysis,
- Data-intensive systems analysis,
- ▶ Self-healing and resilient architecture,
- Assured application programming interface (API) and framework compliance,
- Sociotechnical ecosystems,
- Development environments,
- Trusted computing,
- Specification and verification,
- ▶ Concurrent and distributed systems,
- ▶ Requirements and policy,
- Usable security and privacy,
- Intrusion and malware detection,
- Dynamic network analysis,
- Model checking,
- Secure coding practice,
- Secure process separation, and
- ▶ Verification of cyberphysical systems.

### North Carolina State University SoS lablet

The North Carolina State University (NC State) SoS lablet is housed in the Institute for Next Generation IT Systems and will contribute broadly to the development of an SoS while leveraging NC State's expertise and experience in analytics, including the extensive expertise available in the NC State Institute of Advanced Analytics. The lablet's work draws on several fundamental areas of computing

research and on the related analytics. Some ideas from fault-tolerant computing will be adapted to the context of cybersecurity. Strategies from control theory will be extended to account for the high variation and uncertainty that may be present in systems when they are under attack. Game theory and decision theory principles will be used to explore the interplay between attack and defense. Formal methods will be applied to develop formal notions of cybersecurity resiliency. End-to-end system analysis will be employed to investigate resiliency of large systems against cyberattack. The lablet's work will draw upon ideas from other areas of mathematics, statistics, and engineering. Dr. Laurie Williams is the principal investigator for the NC State SoS lablet.

The NC State SoS lablet projects include

- Understanding attack surface vulnerabilities,
- ▶ Policy complexity and norms,
- ▶ Resilience requirements,
- ▶ Human information processing, and
- Metrics for security models.

### University of Illinois at Urbana-Champaign SoS lablet

The University of Illinois at Urbana-Champaign (UIUC) SoS lablet, housed in the Information Trust Institute, addresses each of the five hard problems. Dr. David M. Nicol, the lablet's principle investigator, explains, "We have a portfolio of projects that will advance the science of security in both experimental and theoretical methodologies, and includes explicit consideration of both mechanized and human elements in SoS models."

The UIUC SoS lablet projects include

- Models and analysis of resiliency to intrusion in cyberphysical systems;
- Models of system and attacker behavior based on data analytics, with application to detecting the presence of intrusion prior to full-scale attack;
- Methodologies for supporting experimental evaluation of network security properties across network layers;

- 2
- Models and analysis of system and human behavior to support decision making in security contexts; and
- A science of human circumvention of security.

#### **University of Maryland SoS lablet**

The University of Maryland (UMD) SoS lablet leverages the resources of the Maryland Cybersecurity Center and brings together 15 UMD faculty from five departments, in collaboration with six external faculty from other universities, to focus on developing scientific foundations of cybersecurity. Principal investigator Dr. Jonathan Katz, professor of computer science and director of the Maryland Cybersecurity Center, says the lablet will "establish mathematical models that can be used to address cybersecurity threats broadly, carry out empirical studies to help validate those models, and develop formal techniques for reasoning about the security of large systems built from multiple components."

Particular research strengths of the lablet include using mathematical and formal tools for studying the verification and composition of security properties; conducting empirical studies based on real-world data about vulnerabilities, exploits, and end-host configurations; and understanding the role of human behavior in cybersecurity, both from the perspectives of honest users as well as attackers. Beyond the research, the lablet will also work to grow the SoS community by sharing its results with the broader public and holding workshops and tutorials.

The UMD SoS lablet projects include

- Verification of hyperproperties;
- ► Trustworthy and composable software systems with contracts;
- Empirical models for vulnerability exploits;
- Human behavior and cyber vulnerabilities;
- Whether the presence of honest users affects intruders' behavior;
- User-centered design for security;
- Understanding developers' reasoning about privacy and security;
- Trust, recommendation systems, and collaboration; and
- Reasoning about protocols with human participants.

The Next Wave is published to disseminate technical advancements and research activities in telecommunications and information technologies. Mentions of company names or commercial products do not imply endorsement by the US Government.

This publication is available online at http://www.nsa.gov/research/tnw/index.shtml. For more information, please contact us at TNW@tycho.ncsc.mil.

